CHAPTER III
MATRIX GROUPS

We begin this chapter by recalling the following notations of matrix groups where F is a field and n is a positive integer :

$G_n(F) =$ the group of nonsingular $n \times n$ matrices over F,

$U_n(F) =$ the group of nonsingular upper triangular $n \times n$ matrices over F,

$L_n(F) =$ the group of nonsingular lower triangular $n \times n$ matrices over F,

$P_n(F) =$ the group of permutation $n \times n$ matrices over F,

$O_n(F) =$ the group of orthogonal $n \times n$ matrices over F,

$V_n(F) =$ the group of all $n \times n$ matrices A over F with $\det A = \pm 1$.

We shall characterize when these matrix groups admit a right nearring structure and a left nearring structure in terms of n and F. The following lemma is our main tool.

Lemma 3.1. *Let G be a group with identity* 1. *If there are distinct $a, b \in G \smallsetminus \{1\}$ such that $a^2 = b^2 = 1$, then $G \notin \mathcal{RNR}$ and $G \notin \mathcal{LNR}$.*

Proof. Suppose that $G \in \mathcal{RNR}$. Since $|G| > 1$, G has no left zero, so there is an operation $+$ on G such that $(G^0, +, \cdot)$ is a right nearring. Then $1 + a = c$ and $1 + b = d$ for some $c, d \in G^0$.

Case 1 : $c \neq 0$. Then $ca = (1 + a)a = a + a^2 = a + 1 = 1 + a = c$. This implies that $a = 1$, a contradiction.

Case 2 : $c = 0$. Then a is an inverse of 1 in $(G^0, +)$. But $b \neq a$, so $1 + b = d \neq 0$. Hence $db = (1 + b)b = b + b^2 = b + 1 = 1 + b = d$ which implies that $b = 1$, a contradiction.

Hence $G \notin \mathcal{RNR}$. We can show similarly that $G \notin \mathcal{LNR}$. □

Theorem 3.2. (i) $G_n(F) \in \mathcal{RNR}$ *if and only if* $n = 1$.
(ii) $G_n(F) \in \mathcal{LNR}$ *if and only if* $n = 1$.

Proof. Assume that $n > 1$. Let $A, B \in M_n(F)$ be defined by

$$A = \begin{bmatrix} 0 & 0 & \cdots & 1 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & \cdots & 0 \end{bmatrix} \text{ and } B = \begin{bmatrix} -1 & 0 & \cdots & 1 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}.$$

Then $A, B \in G_n(F) \smallsetminus \{I_n\}$, $A \neq B$ and $A^2 = I_n = B^2$. By Lemma 3.1, $G_n(F) \notin \mathcal{RNR}$ and $G_n(F) \notin \mathcal{LNR}$. This shows that if $G_n(F) \in \mathcal{RNR}$ or $G_n(F) \in \mathcal{LNR}$, then $n = 1$.

Since $G_1^0(F) = (F \smallsetminus \{0\}, \cdot)^0 = (F, \cdot)$, it follows that $G_1(F) \in \mathcal{R} \subseteq \mathcal{RNR} \cap \mathcal{LNR}$. Hence the converses of (i) and (ii) hold. □

From Theorem 3.2 and its proof, we have

Corollary 3.3. *The following statements are equivalent.*
(i) $G_n(F) \in \mathcal{RNR}$.
(ii) $G_n(F) \in \mathcal{LNR}$.
(iii) $G_n(F) \in \mathcal{R}$.
(iv) $n = 1$.

Theorem 3.4. (i) $U_n(F) \in \mathcal{RNR}$ *if and only if either* $n = 1$ *or* $n = 2$ *and* $F \cong \mathbb{Z}_2$.
(ii) $U_n(F) \in \mathcal{LNR}$ *if and only if either* $n = 1$ *or* $n = 2$ *and* $F \cong \mathbb{Z}_2$.

Proof. Suppose that (1) $n > 1$ and (2) $n > 2$ or $|F| > 2$. This implies that (1′) $n > 2$ or (2′) $n = 2$ and $|F| > 2$.

Case 1 : $n > 2$. Let $A, B \in M_n(F)$ be defined by

$$A = \begin{bmatrix} 1 & 1 & 0 & \cdots & 0 \\ 0 & -1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix} \text{ and } B = \begin{bmatrix} 1 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 1 & 0 & \cdots & 0 \\ 0 & 0 & -1 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 \end{bmatrix}.$$

Then $A, B \in U_n(F) \smallsetminus \{I_n\}$, $A \neq B$ and $A^2 = B^2 = I_n$. By Lemma 3.1, $U_n(F) \notin \mathcal{RNR}$ and $U_n(F) \notin \mathcal{LNR}$.

Case 2 : $n = 2$ and $|F| > 2$. Let $a \in F \smallsetminus \{0, 1\}$ and

$$A = \begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix} \text{ and } B = \begin{bmatrix} 1 & a \\ 0 & -1 \end{bmatrix}.$$

Then $A, B \in U_n(F) \smallsetminus \{I_2\}, A \neq B$ and $A^2 = B^2 = I_2$, so by Lemma 3.1, $U_2(F) \notin \mathcal{RNR}$ and $U_2(F) \notin \mathcal{LNR}$.

This proves that if $U_n(F) \in \mathcal{RNR}$ or $U_n(F) \in \mathcal{LNR}$, then either $n = 1$ or $n = 2$ and $F \cong \mathbb{Z}_2$.

Since

$$U_1^0(F) \cong (F, \cdot) \quad \text{and} \quad U_2^0(\mathbb{Z}_2) \cong \left(\left\{ \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \right\}, \cdot \right)$$
$$\cong (\mathbb{Z}_3, \cdot),$$

it follows that $U_1^0(F), U_2^0(\mathbb{Z}_2) \in \mathcal{R} \subseteq \mathcal{RNR} \cap \mathcal{LNR}$. Then the converses of (i) and (ii) hold. □

As a consequence of Theorem 3.4 and its proof, we have

Corollary 3.5. *The following statements are equivalent.*

(i) $U_n(F) \in \mathcal{RNR}$.

(ii) $U_n(F) \in \mathcal{LNR}$.

(iii) $U_n(F) \in \mathcal{R}$.

(iv) (a) $n = 1$ *or* (b) $n = 2$ *and* $F \cong \mathbb{Z}_2$.

The following theorem and corollary can be shown dually to Theorem 3.4 and Corollary 3.5, respectively.

Theorem 3.6. (i) $L_n(F) \in \mathcal{RNR}$ *if and only if either* $n = 1$ *or* $n = 2$ *and* $F \cong \mathbb{Z}_2$.

(ii) $L_n(F) \in \mathcal{LNR}$ *if and only if either* $n = 1$ *or* $n = 2$ *and* $F \cong \mathbb{Z}_2$.

Corollary 3.7. *The following statements are equivalent.*

(i) $L_n(F) \in \mathcal{RNR}$.

(ii) $L_n(F) \in \mathcal{LNR}$.

(iii) $L_n(F) \in \mathcal{R}$.

(iv) (a) $n = 1$ *or* (b) $n = 2$ *and* $F \cong \mathbb{Z}_2$.

Theorem 3.8. (i) $P_n(F) \in \mathcal{RNR}$ *if and only if* $n \leq 2$.

(ii) $P_n(F) \in \mathcal{LNR}$ *if and only if* $n \leq 2$.

Proof. Assume that $n \geq 3$. Let $A, B \in M_n(F)$ be defined by

$$A = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix} \text{ and } B = \begin{bmatrix} 1 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 \\ 0 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 \end{bmatrix}.$$

Then $A, B \in P_n(F) \smallsetminus \{I_n\}$, $A \neq B$ and $A^2 = B^2 = I_n$. Therefore we have that $P_n(F) \notin \mathcal{RNR}$ and $P_n(F) \notin \mathcal{LNR}$ by Lemma 3.1. Hence $P_n(F) \in \mathcal{RNR}$ or $P_n(F) \in \mathcal{LNR}$ implies that $n \leq 2$.

The converses of (i) and (ii) hold since

$$|P_1(F)| = 1 \quad \text{and} \quad P_2^0(F) \cong \left(\left\{\begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix}, \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}, \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\right\}, \cdot\right) \cong (\mathbb{Z}_3, \cdot).$$

□

We have the following consequence, as before.

Corollary 3.9. *The following statements are equivalent.*

(i) $P_n(F) \in \mathcal{RNR}$.

(ii) $P_n(F) \in \mathcal{LNR}$.

(iii) $P_n(F) \in \mathcal{R}$.

(iv) $n \leq 2$.

Theorem 3.10. (i) $O_n(F) \in \mathcal{RNR}$ *if and only if either* $n = 1$ *or* $n = 2$ *and* $F \cong \mathbb{Z}_2$.

(ii) $O_n(F) \in \mathcal{LNR}$ *if and only if either* $n = 1$ *or* $n = 2$ *and* $F \cong \mathbb{Z}_2$.

Proof. Suppose that (1) $n > 1$ and (2) $n > 2$ or $|F| > 2$. Then (1′) $n > 2$ or (2′) $n = 2$ and $|F| \geq 3$.

Case 1 : $n > 2$. Let $A, B \in M_n(F)$ be as in the proof of Theorem 3.8. Since $A^t = A$ and $B^t = B$, we have that $AA^t = A^2 = I_n$ and $BB^t = B^2 = I_n$. Then $A, B \in O_n(F) \smallsetminus \{I_n\}$, $A \neq B$ and $A^2 = B^2 = I_n$. By Lemma 3.1, $O_n(F) \notin \mathcal{RNR}$ and $O_n(F) \notin \mathcal{LNR}$.

Case 2 : $n = 2$ and $|F| \geq 3$.

Subcase 2.1 : $\operatorname{char} F = 2$. Let $a \in F \smallsetminus \{0, 1\}$. Let

$$A = \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix} \text{ and } B = \begin{bmatrix}a & 1+a\\ 1+a & a\end{bmatrix}.$$

Then $A^t = A$ and $B^t = B$, so $AA^t = A^2 = I_2$ and

$$BB^t = B^2 = \begin{bmatrix}a^2 + (1+a)^2 & a(1+a) + (1+a)a\\ (1+a)a + a(1+a) & (1+a)^2 + a^2\end{bmatrix} = \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$$

หอสมุดกลาง สถาบันวิทยบริการ จุฬาลงกรณ์มหาวิทยาลัย

since char$F = 2$. Hence A and B are two distinct elements of $O_2(F)$ with $A^2 = B^2 = I_2$. Thus $O_2(F) \notin \mathcal{RNR}$ and $O_2(F) \notin \mathcal{LNR}$ by Lemma 3.1.

Subcase 2.2 : char$F \neq 2$. Then $\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$ and $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ are distinct elements of $O_2(F)$ whose squares are I_2. Hence $O_2(F) \notin \mathcal{RNR}$ and $O_2(F) \notin \mathcal{LNR}$ by Lemma 3.1.

This proves that if $O_2(F) \in \mathcal{RNR}$ or $O_2(F) \in \mathcal{LNR}$, then either $n = 1$ or $n = 2$ and $F \cong \mathbb{Z}_2$.

We have that

$$O_1^0(F) \cong (\{0, 1, -1\}, \cdot) \cong \begin{cases} (\mathbb{Z}_3, \cdot) & \text{if char} F \neq 2, \\ (\mathbb{Z}_2, \cdot) & \text{if char} F = 2. \end{cases}$$

and

$$O_2^0(\mathbb{Z}_2) \cong \left(\left\{ \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\}, \cdot \right) \cong (\mathbb{Z}_3, \cdot).$$

These imply that $O_1^0(F), O_2^0(\mathbb{Z}_2) \in \mathcal{R} \subseteq \mathcal{RNR} \cap \mathcal{LNR}$. Hence the converses of (i) and (ii) hold. □

As before, Theorem 3.10 and its proof yield the following result.

Corollary 3.11. *The following statements are equivalent.*

(i) $O_n(F) \in \mathcal{RNR}$.

(ii) $O_n(F) \in \mathcal{LNR}$.

(iii) $O_n(F) \in \mathcal{R}$.

(iv) (a) $n = 1$ *or* (b) $n = 2$ *and* $F \cong \mathbb{Z}_2$.

Theorem 3.12. (i) $V_n(F) \in \mathcal{RNR}$ *if and only if* $n = 1$.

(ii) $V_n(F) \in \mathcal{LNR}$ *if and only if* $n = 1$.

Proof. Assume that $n > 1$ and let $A, B \in M_n(F)$ be defined as in the proof of Theorem 3.2. Since $\det A = -1 = \det B$, it follows that $A, B \in V_n(F)$. Then

$A, B \in V_n(F) \setminus \{I_n\}, A \neq B$ and $A^2 = B^2 = I_n$. Hence by Lemma 3.1, $V_n(F) \notin \mathcal{RNR}$ and $V_n(F) \notin \mathcal{LNR}$.

Since

$$V_1^0(F) \cong (\{0, 1, -1\}, \cdot) \cong \begin{cases} (\mathbb{Z}_3, \cdot) & \text{if char} F \neq 2, \\ (\mathbb{Z}_2, \cdot) & \text{if char} F = 2, \end{cases}$$

we have that $V_1^0(F) \in \mathcal{R} \subseteq \mathcal{RNR} \cap \mathcal{LNR}$.

Therefore the theorem is proved. $\square$

From Theorem 3.12 and its proof, we also have

Corollary 3.13. *The following statements are equivalent.*

(i) $V_n(F) \in \mathcal{RNR}$.

(ii) $V_n(F) \in \mathcal{LNR}$.

(iii) $V_n(F) \in \mathcal{R}$.

(iv) $n = 1$.

Remark 3.14. Let K be a subfield of F and

$$W_n(F, K) = \{A \in M_n(F) \mid \det A \in K \setminus \{0\}\}.$$

Then $W_n(F, K)$ is a group. Since $1, -1 \in K$, it follows from the proof of Theorem 3.12 that if $W_n(F, K) \in \mathcal{RNR}$ or $W_n(F, K) \in \mathcal{LNR}$, then $n = 1$. Also, we have that

$$W_1^0(F, K) \cong (K, \cdot) \in \mathcal{R} \subseteq \mathcal{RNR} \cap \mathcal{LNR}.$$

Therefore we deduce that $n = 1$ is necessary and sufficient for $W_n(F, K)$ to be in $\mathcal{RNR}$ [$\mathcal{LNR}$]. Moreover, the conditions that $W_n(F, K) \in \mathcal{RNR}$, $W_n(F, K) \in \mathcal{LNR}$, $W_n(F, K) \in \mathcal{R}$ and $n = 1$ are equivalent.